БАНКОВСКИЙ ПРОЦЕССИНГОВЫЙ ЦЕНТР

ОТЧЕТ

о тенденциях и случаях мошенничества в сфере платежных инструментов и сервисов за 2022 год

Отчет подготовлен ОАО «Банковский процессинговый центр» на основании имеющейся информации по операциям с банковскими платежными карточками. Данные не охватывают всю территорию Республики Беларусь, однако, учитывая долю рынка ОАО «Банковский процессинговый центр», могут свидетельствовать об основных тенденциях в Республике Беларусь. **При сравнении данных в абсолютных значениях используются значения в условных единицах.**

Общая информация:

Основная доля мошенничества в Республике Беларусь в 2022 году, как и в прошлом году, приходится на мошенничество с банковскими платежными карточками в среде без физического присутствия держателя карточки при проведении операции, в частности на мошенничество с применением методов социальной инженерии. Случаев установки скимминговых устройств и массовой компрометации данных держателей карточек на территории Республики Беларусь в 2022 году зафиксировано не было.

Эмиссия (данные по операциям с банковскими платежными карточками, выпущенными банками, которые обслуживаются в ОАО «Банковский процессинговый центр»):

Характерной тенденцией 2022 года является мошенничество с использованием реквизитов карточек наряду с единичными случаями мошенничества по поддельным и утерянным/украденным карточкам. В среде мошенничества с использованием реквизитов карточек основная доля мошенничества приходится на социальную инженерию – около 82%. Значительная доля мошенничества с применением социальной инженерии свидетельствует о том, что данный вид мошенничества адаптируется к любым условиям, а использование методов социальной инженерии приносит достаточно высокий доход злоумышленникам, при этом не требует серьезных финансовых вложений. Мошенники стремятся получить личные данные держателей карточек, доступы к их счетам, системам дистанционного банковского обслуживания, МСИ и мобильным устройствам.

Хранящиеся на карточных счетах денежные средства – традиционно привлекательная цель для кибермошенников. В связи с этим злоумышленники регулярно атакуют клиентов банков с использованием фишинга и социальной инженерии. Держатели банков, подключенных к Центру, в 2022 году сталкивались с мошенничеством или обманом, в результате которого злоумышленники выманивали деньги, данные карточек, логины и пароли интернет-банкинга. Основными способами коммуникации мошенников с держателями карточек в 2022 году в Республике Беларусь являлись торговые площадки, звонки от имени банковских, финансовых и других организаций, фишинговые письма, а также сообщения в социальных сетях.

Мошенники постоянно выстраивают новые схемы используя актуальную повестку для того чтобы не вызывать подозрений у рядовых пользователей платежных инструментов. Характерными для

2022 года являются звонки держателям или рассылка информационных сообщений от имени банков в мессенджерах о возможной блокировке мобильного приложения банка в официальных магазинах с рекомендацией установить новое приложение на мобильный телефон. Как правило, под видом банковского приложения злоумышленники устанавливают на мобильные устройства граждан приложения удаленного доступа и получают полный контроль над их счетами и денежными средствами. Наиболее популярными среди данных приложений являются AnyDesk и TeamViewer. Еще одним из вариантов схемы мошенничества после установки программ удаленного доступа на телефон держателя является использование мобильного банкинга банков Республики Беларусь. После получения доступа к учетным записям мобильного приложения банка злоумышленники открывают виртуальные карточки и используют их в качестве промежуточного звена для вывода денежных средств, заработанных преступным путем, в свою очередь, держатели могут даже не подозревать о том, что на их имя выпущены карточки в каком-либо банке.

В 2022 году злоумышленники активно использовали схемы мошенничества с оформлением кредита. Существуют различные алгоритмы, направленные на получение персональных данных клиентов для дальнейшего оформления кредитной линии, например, мошенник может представиться работником банка, в ходе разговора сообщить, что со счета держателя пытаются вывести деньги, а для того чтобы спасти финансовые средства необходимо открыть кредитную линию и сообщить реквизиты своего счёта. Также злоумышленники, выдающие себя за работников банка, могут просить устанавливать специальные приложения на телефон для лучшей защиты - упомянутые выше программы удаленного доступа.

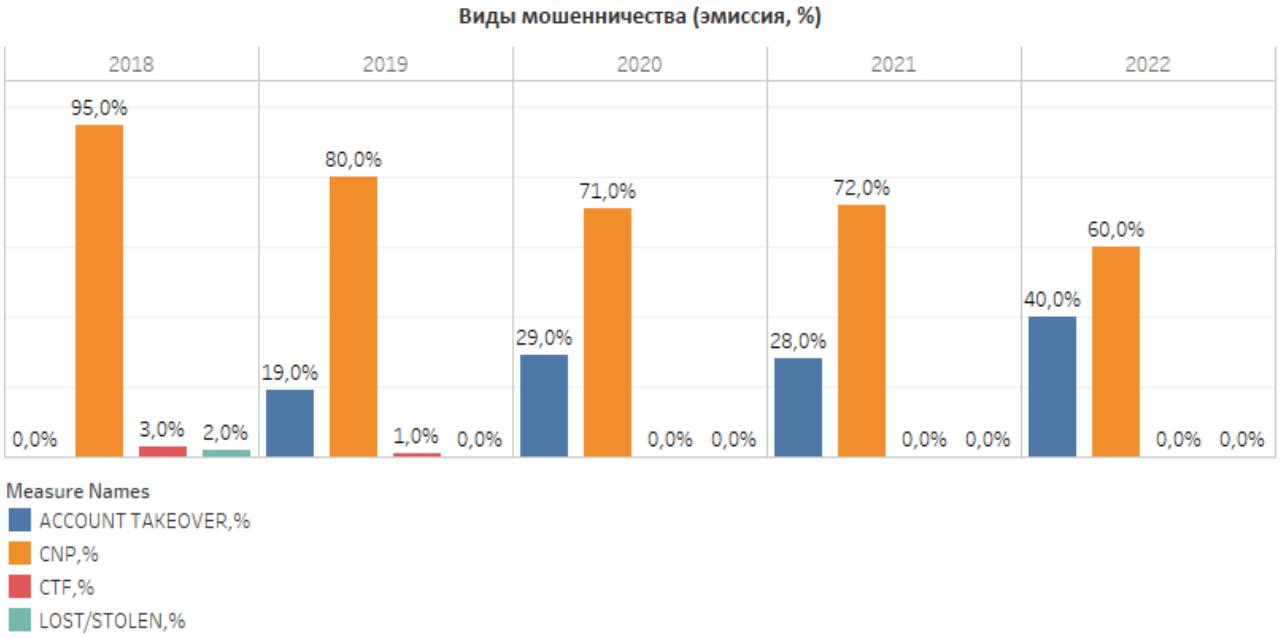
Известны случаи и звонков от псевдо-сотрудников правоохранительных органов. Неизвестные, как правило, обращаются к держателю по имени и фамилии, но при этом уточняют дополнительные персональные данные: идентификационный номер паспорта, место и стаж работы, уровень заработной платы и т.д., таким образом они получают достаточно личных данных для оформления кредита. В случае потери бдительности и следованию заранее разработанному мошенниками алгоритму, граждане вынуждены погашать оформленный на них кредит.

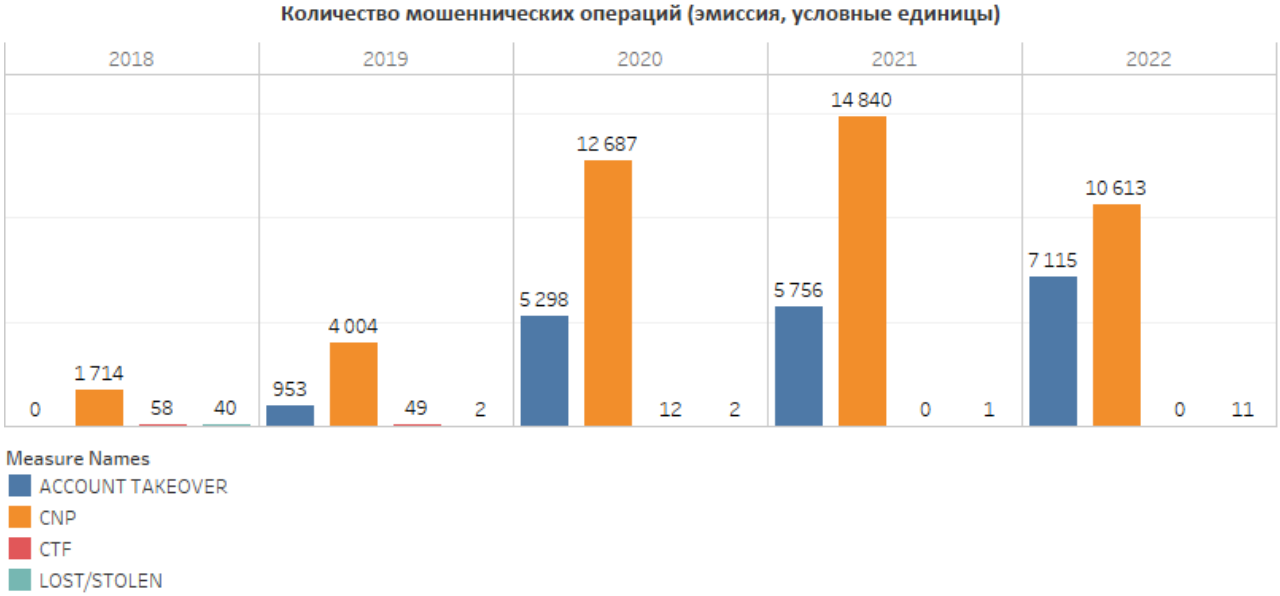
В 2022 году участились и случаи использования схемы мошенничества, связанной с сайтами знакомств, когда злоумышленники для якобы организации встречи присылают держателям фишинговые ссылки на покупку билетов в театр или кино. В случае, если клиент переходит по данной ссылке и соглашается с проведением оплаты, с его счета списывается значительная сумма.

По итогам 2022 года количество мошеннических операций по карточкам банков, которые обслуживаются в ОАО «Банковский процессинговый центр», по типу мошенничества распределилось следующим образом: **60%** мошеннических операций приходится на мошенничество **с использованием реквизитов карточек**, **40%** незаконных операций с банковскими платежными карточками приходится на **account takeover (перехват счета),** успешных мошеннических операций с использованием **поддельных карточек** не зафиксировано.

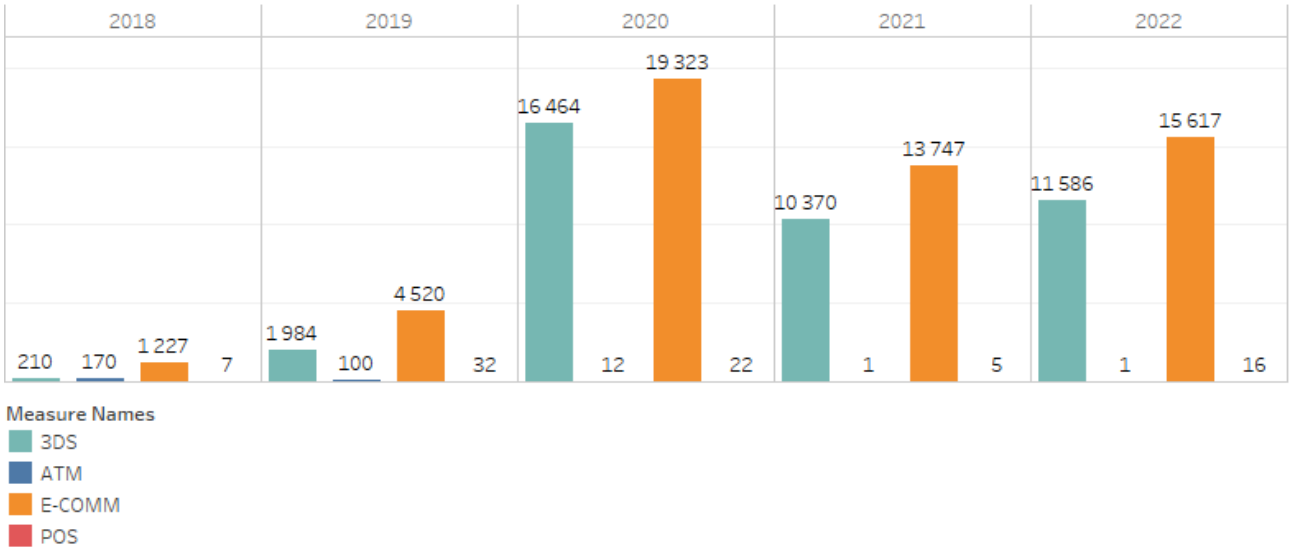
В 2022 году количество выявленных мошеннических случаев (карточек) увеличилось относительно 2021 года на 14%, но при этом по сравнению с 2021 годом на 14% сократилось общее количество успешных мошеннических операций, заявленных в международные платежные системы, общая сумма успешных мошеннических операций уменьшилась на 15%, а средняя сумма 1 мошеннической операции составила 42 доллара США, что соответствует аналогичному показателю прошлого года. Уменьшение общей суммы успешных мошеннических операций, заявленных в международные платежные системы обусловлено изменением геополитической ситуации в начале 2022 года и переориентацией злоумышленников на использование платежных сервисов, которые зарегистрированы на территории Республики Беларусь.

Детальная информация о тенденциях мошенничества представлена на диаграммах ниже.

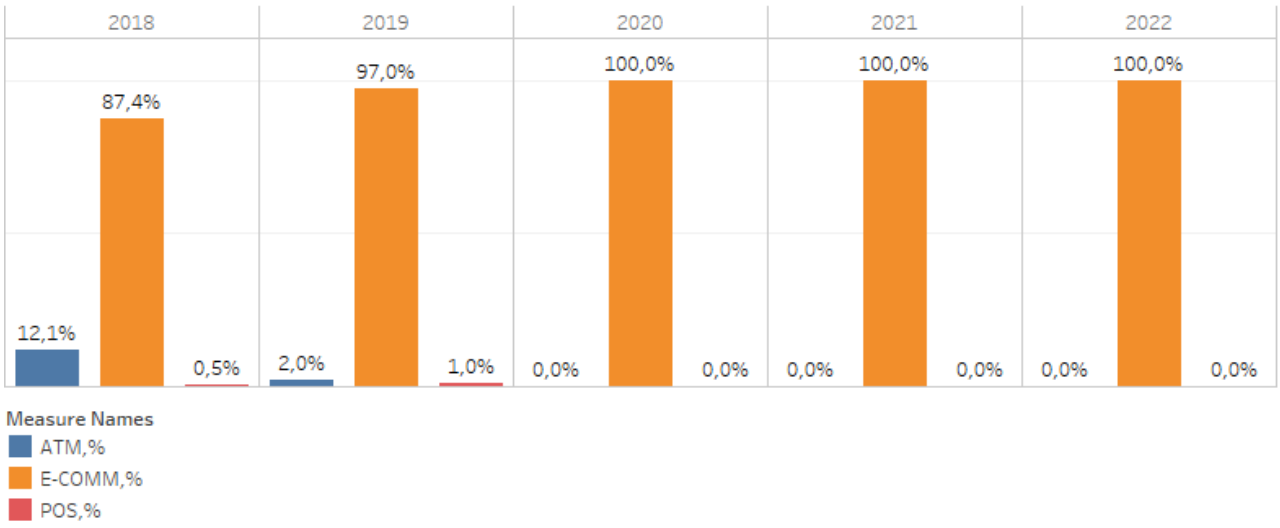


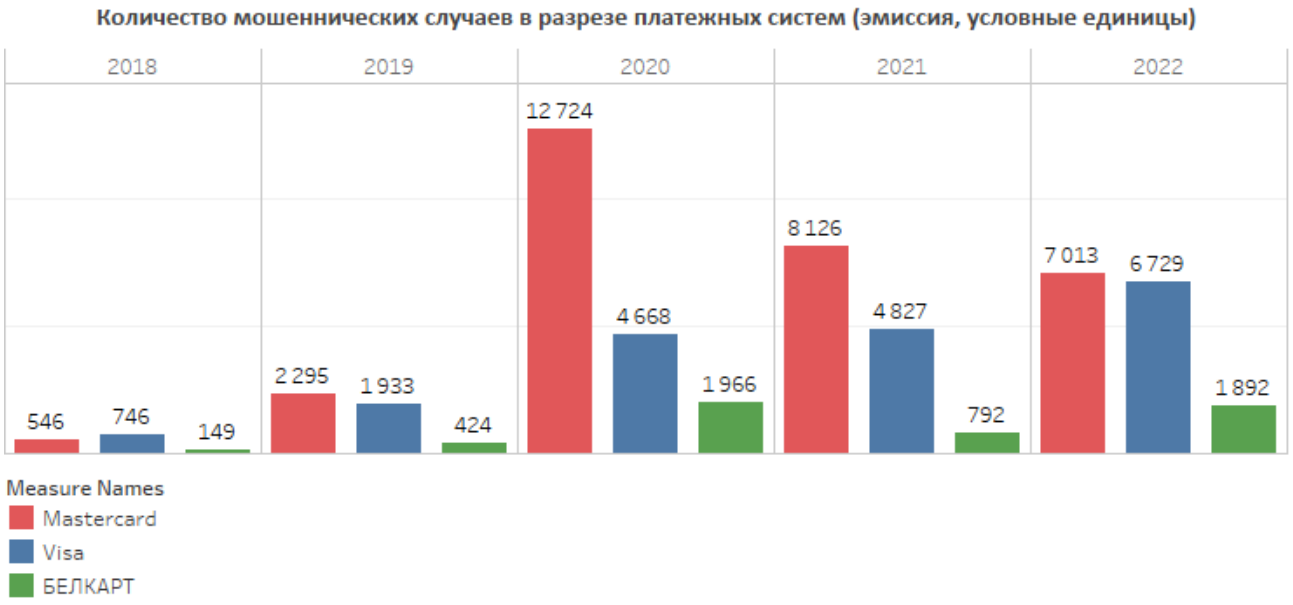


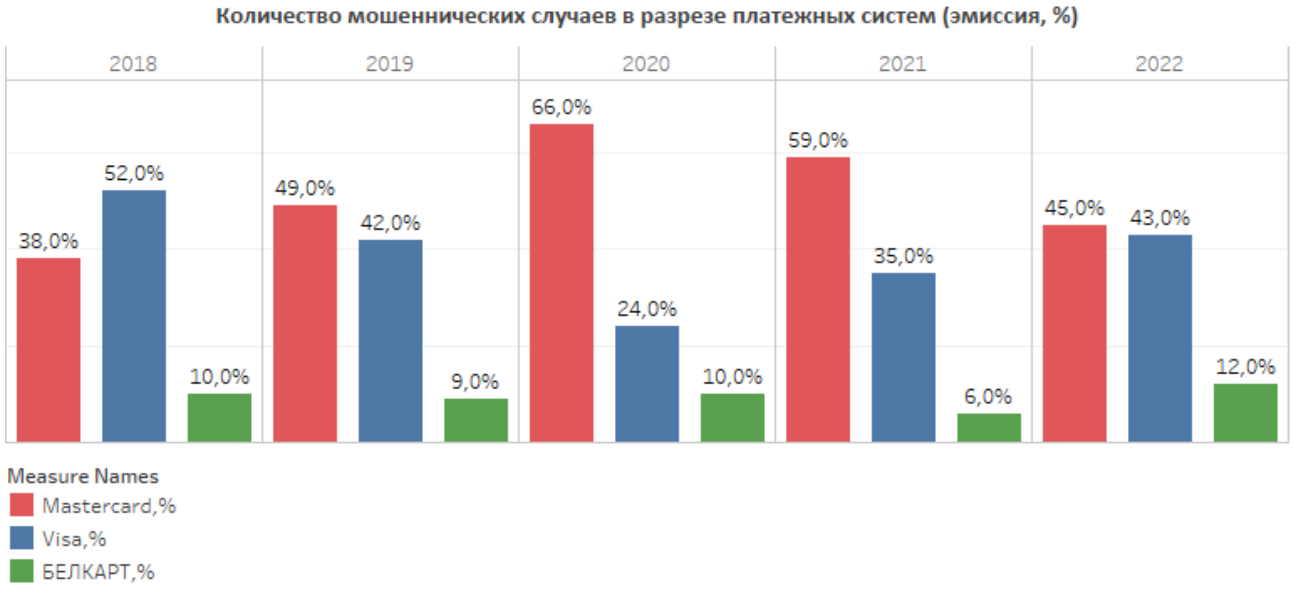
Количество мошеннических случаев в разрезе мест их совершения (эмиссия, условные единицы)



Количество мошеннических случаев в разрезе мест их совершения (эмиссия, %)



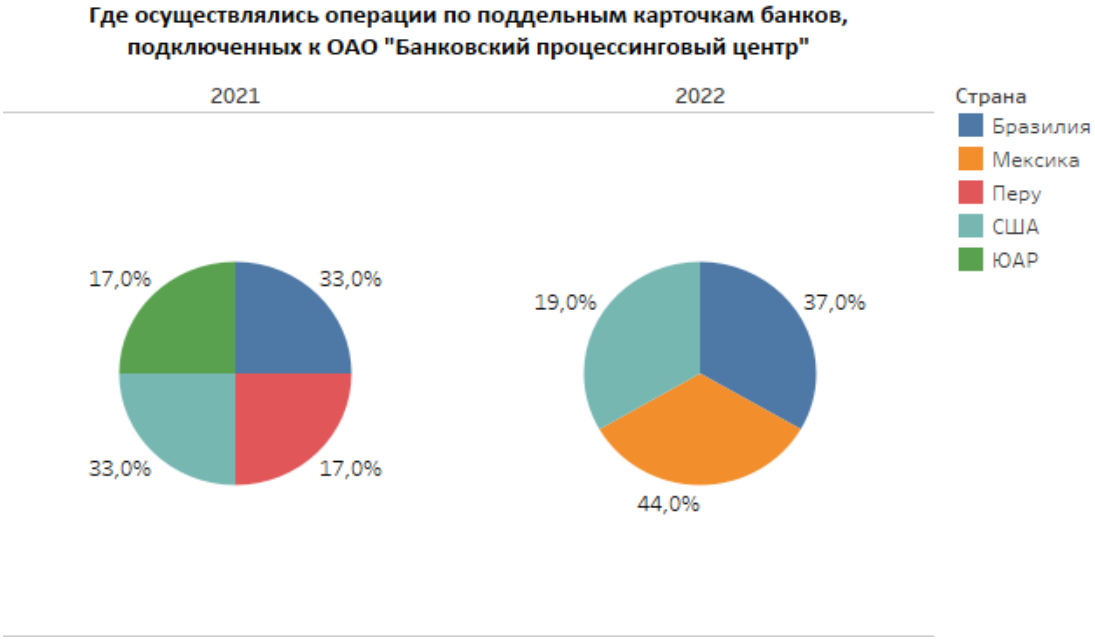




Операции по поддельным карточкам:

В 2022 году количество попыток мошеннических операций с использованием поддельных карточек увеличилось в 2,7 раза относительно 2021 года за счет использования реквизитов карточек, по которым проходили сгенерированные мошенниками попытки проведения операций по магнитной полосе. Был зафиксирован один случай использования поддельной карточки в АТМ в США (вероятно компрометация произошла на территории Бразилии), в 2021 году также был зафиксирован всего один случай использования поддельной карточки в АТМ в Южно-Африканской Республике, где карточка и была скомпрометирована.

В рамках использования поддельных карточек в ОТС в 2022 году были выявлены случаи неуспешных попыток проведения сгенерированных мошенниками операций с использованием магнитной полосы в ОТС Бразилии и Мексики, а также случай неуспешной попытки использования поддельной карточки в ресторане быстрого питания и в супермаркете на территории США.



Мошеннические операции с использованием реквизитов карточек:

Основными тенденциями мошенничества с использованием реквизитов карточек в 2022 году являются:

- мошенничество с применением методов социальной инженерии, обусловленное компрометацией реквизитов карточек клиентов преимущественно посредством взаимодействия мошенников с держателями на торговых площадках, а также scam звонков держателям. Действия мошенников направлены на выманивание необходимых реквизитов у держателей с целью дальнейшего вывода средств. В 2022 году злоумышленники для вывода денежных средств преимущественно использовали платежные сервисы, которые зарегистрированы на территории Республики Беларусь, так как ограничения, введенные международными платежными системами в связи с изменениями геополитической ситуации, исключили возможность использования онлайн-сервисов, зарегистрированных на территории Российской Федерации. В свою очередь эти изменения также повлияли на увеличение доли ОТС, зарегистрированных на территории РБ, в которых осуществлялись мошеннические операции с использованием реквизитов карточек. В целом, в 2022 году наблюдался рост в 1,2 раза случаев мошенничества с использованием социальной инженерии относительно 2021 года;

- наличие фактов компрометации систем дистанционного банковского обслуживания клиентов посредством социальной инженерии. Особую ценность для злоумышленников имеют такие данные, как логины/пароли и доступы к системам ДБО, перехват которых способствует получению полного управления финансами держателя. Все чаще получение доступа к системам ДБО клиента осуществляется путем установки злоумышленниками на мобильное устройство держателя программ удаленного доступа;

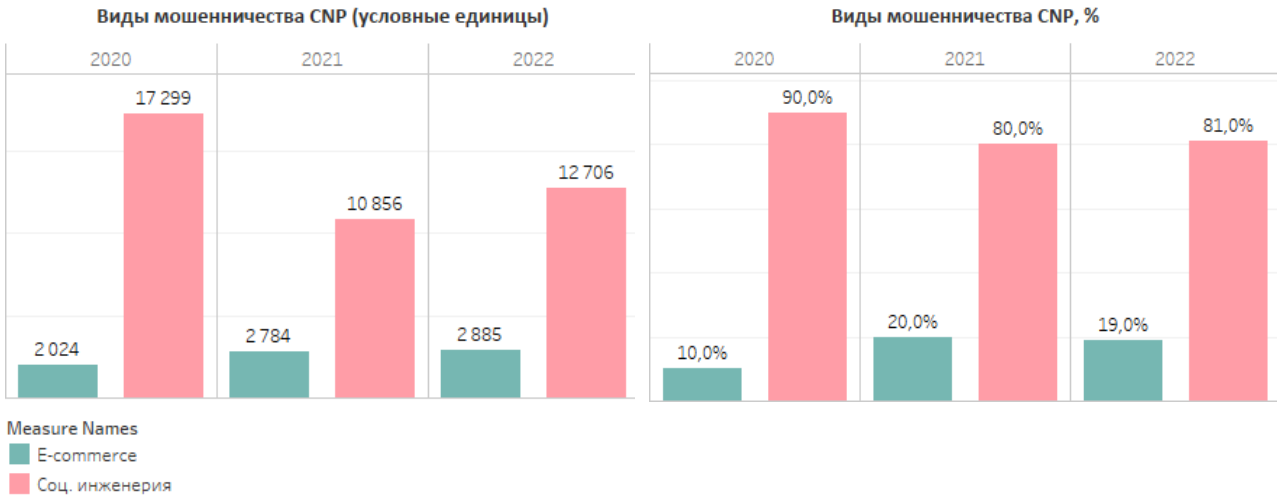
- увеличение случаев мошенничества в среде e-commerce, обусловленное компрометацией реквизитов карточек держателей. Так в 2022 году наблюдался рост данного вида мошенничества на 4% по сравнению с 2021 годом;

- наличие мошеннических операций на онлайн-сервисах, которые занимаются продажей цифровых товаров: компьютерных программ, игр и приложений. Мошенничество связано со взломом аккаунтов учетной записи Google реальных пользователей, после чего злоумышленники осуществляют большое количество операций оплаты на различных Google-сервисах. Данные сервисы, как правило, зарегистрированы на территории США и Великобритании, что объясняет высокую долю операций с использованием реквизитов карточек в ОТС, зарегистрированных на территории США и Великобритании в текущем году;

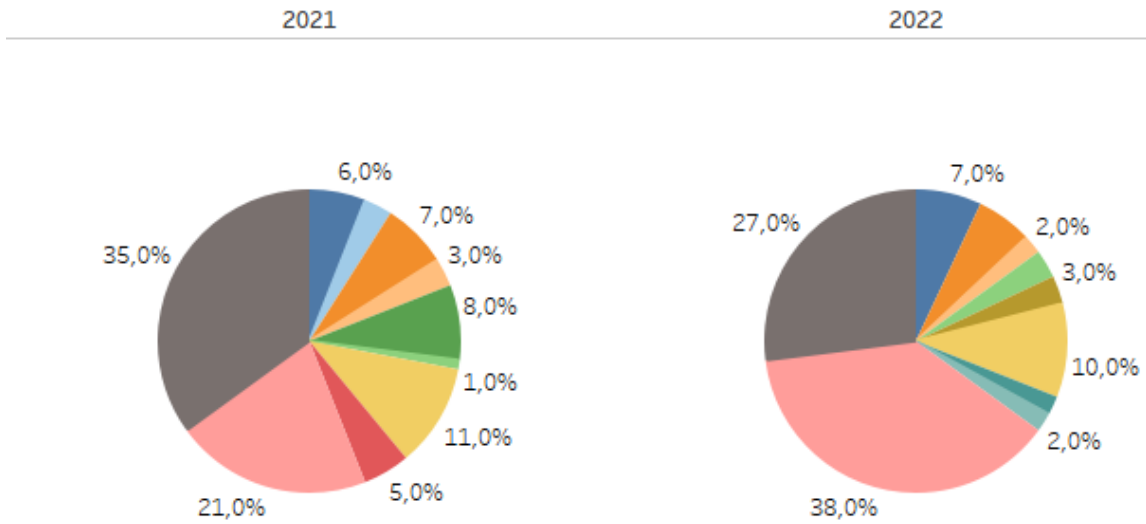
- практическое снижение до минимума случаев мошенничества с использованием токенов. После прекращения деятельности международных платежных систем Visa и Mastercard на территории России данный вид мошенничества значительно сократился (в 13 раз относительно 2021 года) в связи с невозможностью его реализации в настоящих условиях. Однако в случае мошенничества по токенам злоумышленники привязывают токен карточки держателя на свое мобильное устройство и совершают несанкционированные платежи с использованием заведенного электронного кошелька в сети Интернет (62% случаев в 2022 году), в ОТС и в банкоматах (1 случай использования токена в банкомате на территории Украины был зарегистрирован в 1 квартале 2022 года);

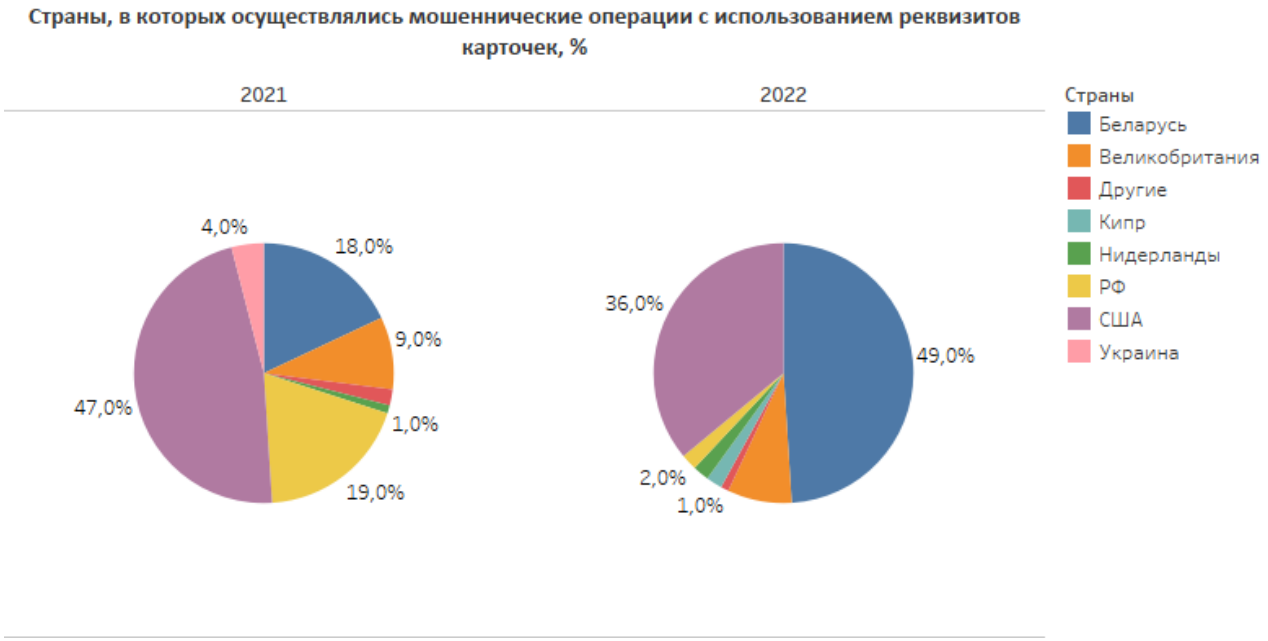
- снижение количества мошеннических тестовых операций и атак на БИНы банков (сгенерированные номера карточек) с целью выявления реальных карточек для дальнейшего использования их реквизитов в мошеннических целях. Для данных операций в 2022 году чаще использовались ОТС, зарегистрированные на территории США и Кипра;

- присутствие фактов «friendly fraud» мошенничества, при котором владелец карточки либо его родственники/знакомые оплачивают товар или услугу, получают его/ее, пользуются, а затем намеренно инициируют возврат платежа, утверждая, что данные их карточки были скомпрометированы.



Категории ОТС, в которых проводились мошеннические операции с использованием реквизитов карточек, %





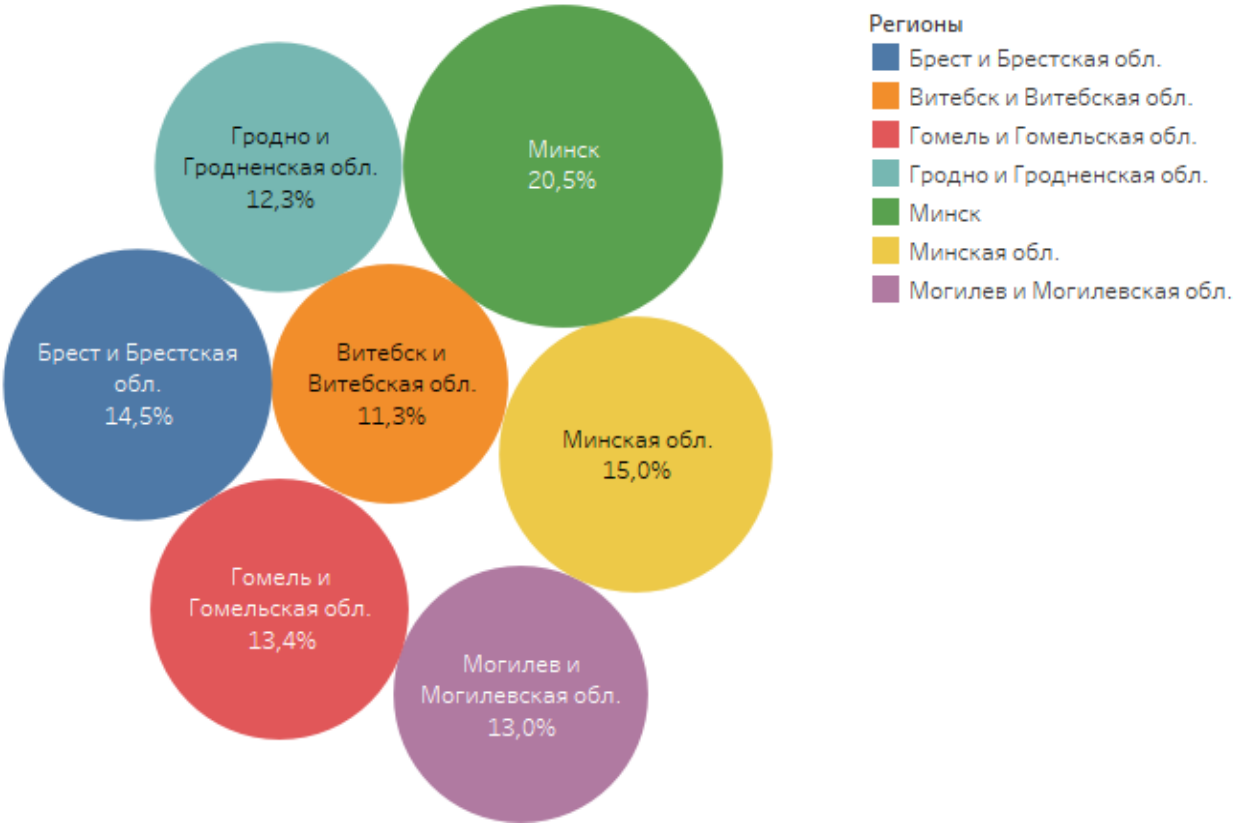
Статистика держателей, подвергшихся мошенничеству:

Согласно аналитическим данным ОАО «Банковский процессинговый центр» в 2022 году более доверчивыми оказались женщины - 57% случаев. В 20,5% случаев держатели, проживающие в городе Минске, стали жертвами злоумышленников, а 79,5% случаев мошенничества приходится на клиентов, проживающих в остальных регионах Беларуси.

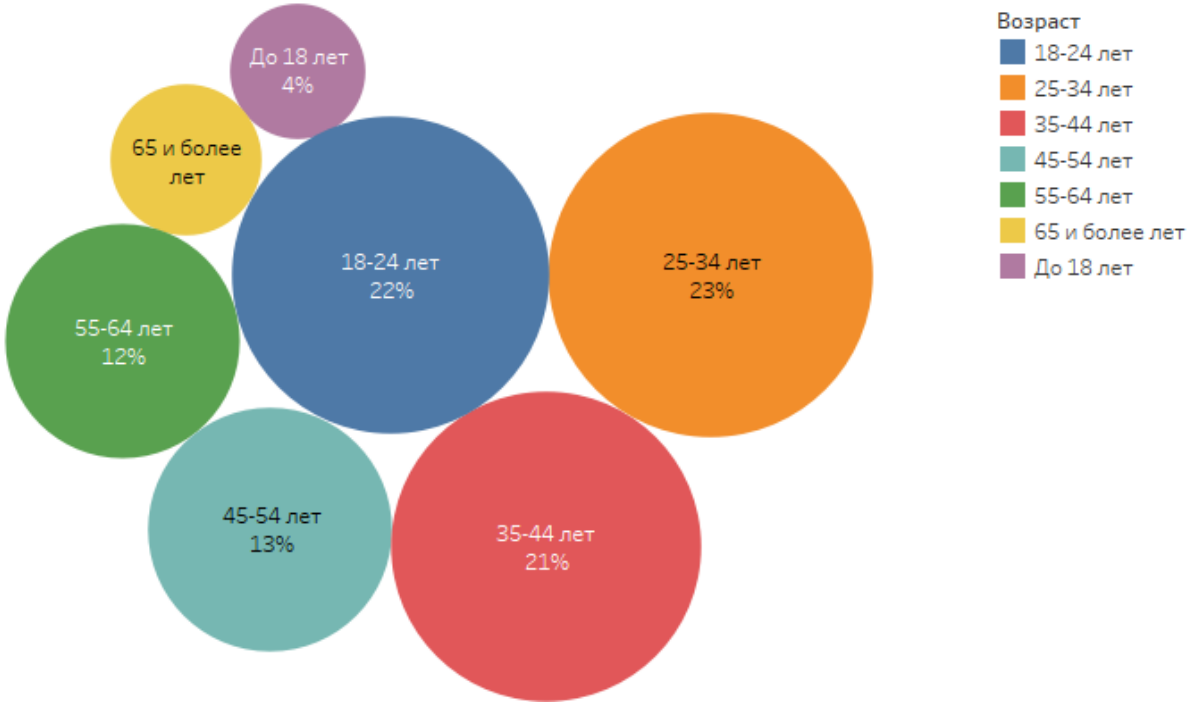
В 91% случаев мошенничество направлено на экономически активных граждан в возрасте от 18 до 64 лет, 5% – на держателей старше 65 лет, 4% атак пришлось на держателей младше 18 лет.

Детальная информация представлена на диаграммах.

Распределение держателей по регионам,%



Распределение держателей по возрасту, %

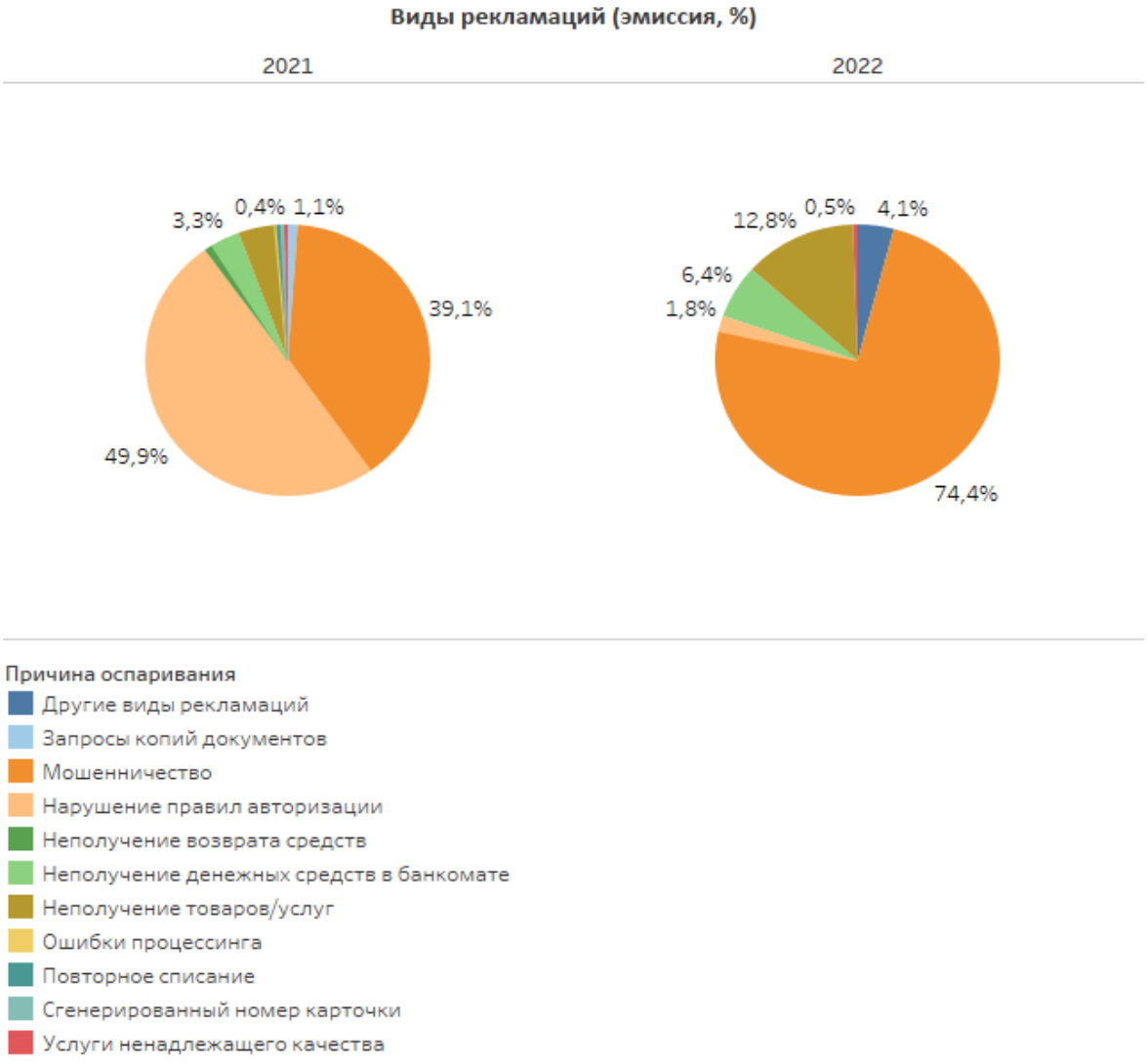


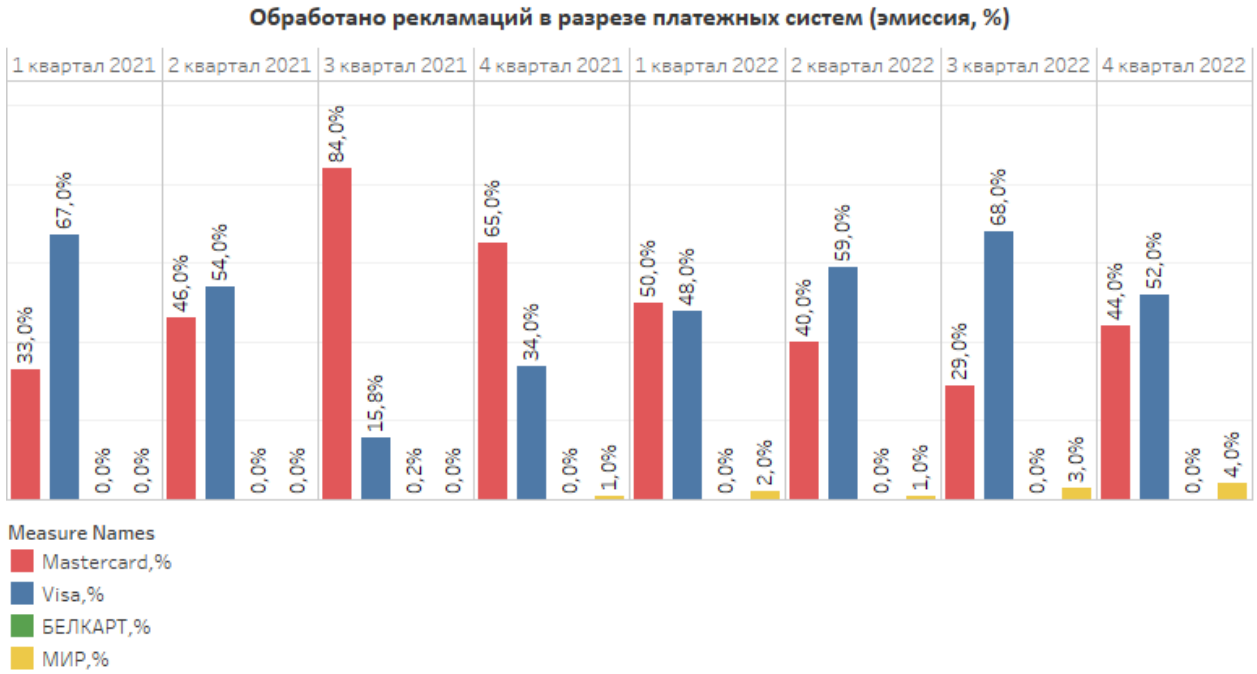
Рекламации эмиссия (данные по операциям с банковскими платежными карточками, выпущенными банками, которые обслуживаются в ОАО «Банковский процессинговый центр»):

В 2022 году общее количество рекламаций снизилось более чем в 2,3 раза. Важно отметить, что наибольшее влияние на снижение количества обработанных эмитентских рекламаций в 2022 году по сравнению с 2021 годом оказало значительное количество рекламаций, инициированных по причине нарушения правил авторизации из-за технического сбоя, произошедшего в 2021 году на стороне банка-эквайера Adyen, обслуживающего приложение Google (35% от всех исходящих рекламаций в 2021 году).

С 01.04.2022 МПС Visa и Mastercard не позволяют процессировать любые этапы рекламаций в адрес банков-резидентов РФ, находящихся под санкциями. При этом МПС Visa распространила ограничения не только на банки-резиденты РФ - блокировка охватывает и транзакции по карточкам, выпущенным и обслуживаемым в финансовых учреждениях за пределами РФ, но проведенные на территории РФ.

Детальная информация представлена на диаграммах ниже.





Эквайринг (данные по операциям в эквайринговой сети банков, подключенных к ОАО «Банковский процессинговый центр»):

В 2022 году в 2 раза выросло количество операций мошеннического характера в эквайринговой сети банков, которые обслуживаются в ОАО «Банковский процессинговый центр». **50%** составляют мошеннические операции **без присутствия карточки** (40% из них - это операции с использованием 3 - D Secure, 44% - COF-транзакции); **33%** приходится на долю мошеннических операций **по утерянным/украденным карточкам; 11%** приходится на **другие виды мошенничества:** 65% из них incorrect processing – на стороне эмитента были спроцессированы некорректные параметры (заявленные операции прошли по признаку бесконтактных операций); 28% составляет account takeover – мошенничество, при котором осуществляется перехват данных держателей и, получая контроль над счетом, мошенники совершают безаутентификационные операции (социальная инженерия); 7% - мошенничество, связанное с выпуском карточки по поддельным данным; **6%** приходится на мошеннические операции с использованием **поддельных карточек**.

Мошеннические операции по **утерянным/украденным карточкам** в 89% случаев были осуществлены с признаком проведения бесконтактных операций, в 6% случаев осуществлялись с использованием чипа EMV, 5% пришлось на операции с использованием реквизитов карточек. Бесконтактные операции позволяют мошенникам совершать большое количество операций в рамках установленных лимитов без необходимости подтверждения совершения операции ПИН-кодом либо использования других методов подтверждения авторизации.

Мошенничество по **поддельным карточкам** в 58% случаев проходило по бесконтактному признаку, 40% из заявленных операций прошли с использованием реквизитов карточек, 2% - с использованием технологии EMV. Реальных случаев использования поддельных карточек в эквайринге банков, подключенных к ОАО «Банковский процессинговый центр», в 2022 году не было зафиксировано.

Общая сумма успешных мошеннических операций по сравнению с 2021 годом увеличилось в 1,8 раза, средняя сумма 1 мошеннической операции составила 84 доллара США (91 доллар США в 2021 году).

Снижение средней суммы мошеннической операции в 2022 году обусловлено наличием большого количества мошеннических COF-транзакций, по которым, как правило, проходили списания на небольшие суммы, что обусловлено спецификой деятельности ОТС, в которых используется данный вид оплаты.

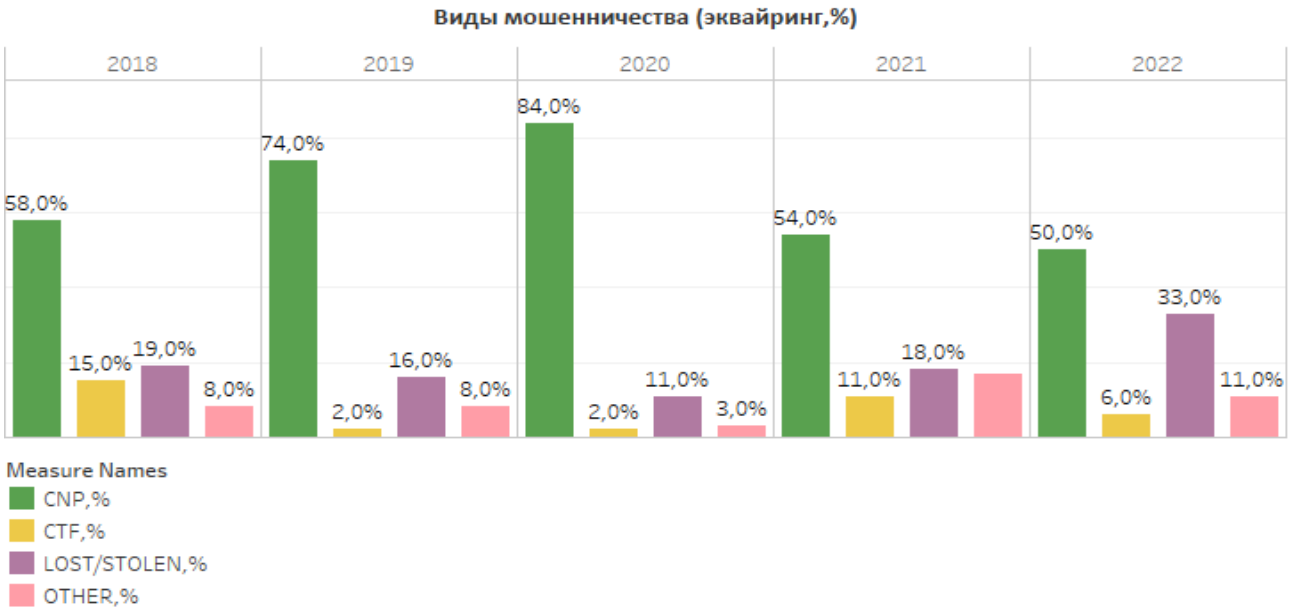
Топ MCC, в которых осуществлялись мошеннические операции в эквайринге, распределился следующим образом: 25% мошеннических операций прошли в продовольственных магазинах и супермаркетах; 16% в сфере общественного питания, барах и ресторанах; 10% пришлось на сервисы, которые занимаются услугами по компьютерному программированию, обработке данных и проектированию; 8% - ОТС, предоставляющие развлекательные услуги; 7% - услуги платного телевидения; по 5% на телекоммуникационные услуги и автозаправочные станции; 4% - авиакомпании; по 2% на профессиональные услуги и услуги такси и 16% - другие ОТС.

Наиболее часто в 2022 году в эквайринговой сети в мошеннических целях использовались карточки банков, эмитированных банками США, России, Великобритании и Италии.

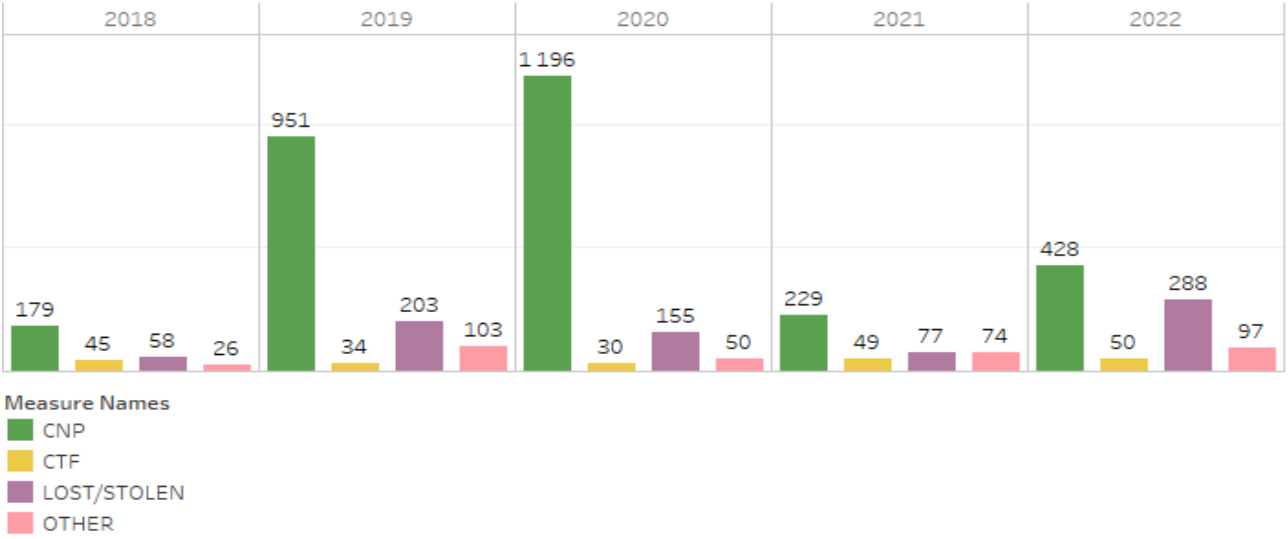
Количество случаев мошеннических операций без присутствия карточки в 2022 году увеличилось относительно 2021 года в 2 раза. Развитие информационных технологий, совершенствование систем защиты банкоматов, постепенный выход из оборота карточек только с магнитной полосой, а также незначительные затраты злоумышленников при мошенничестве в среде без присутствия карточки – все это способствует снижению уровня мошенничества по поддельным карточкам.

В 4 квартале 2022 года впервые были зафиксированы мошеннические операции по карточкам ПС «Мир». 84% случаев заявленного мошенничества по карточкам ПС «Мир» прошли с признаком бесконтактных операций. По карточкам платежной системы UnionPay Intarnational в эквайринговой сети не было зафиксировано ни одной мошеннической операции.

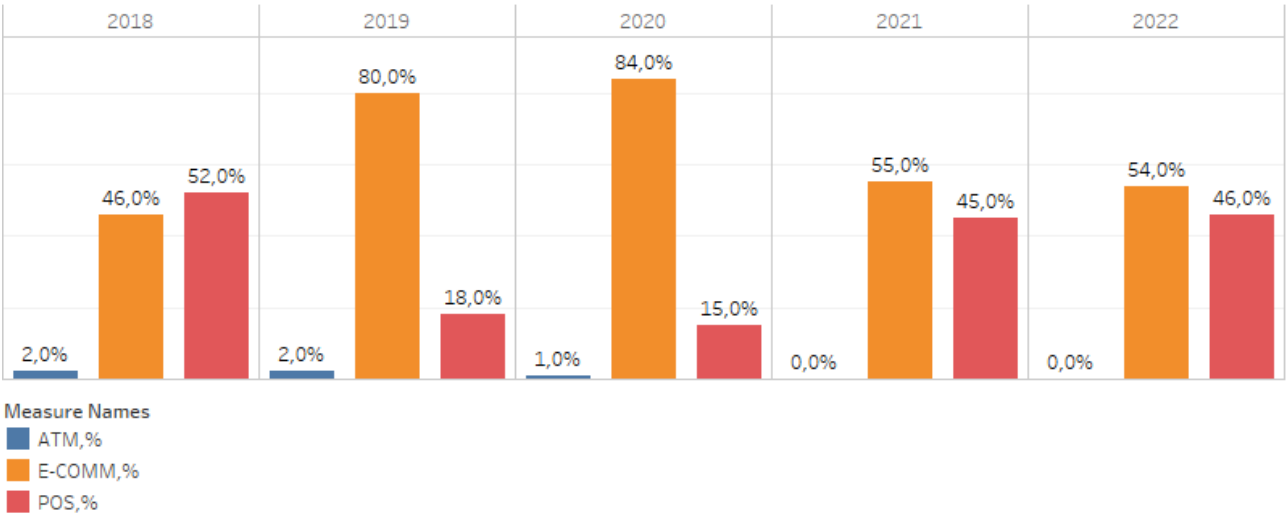
Детальная информация представлена на диаграммах ниже.



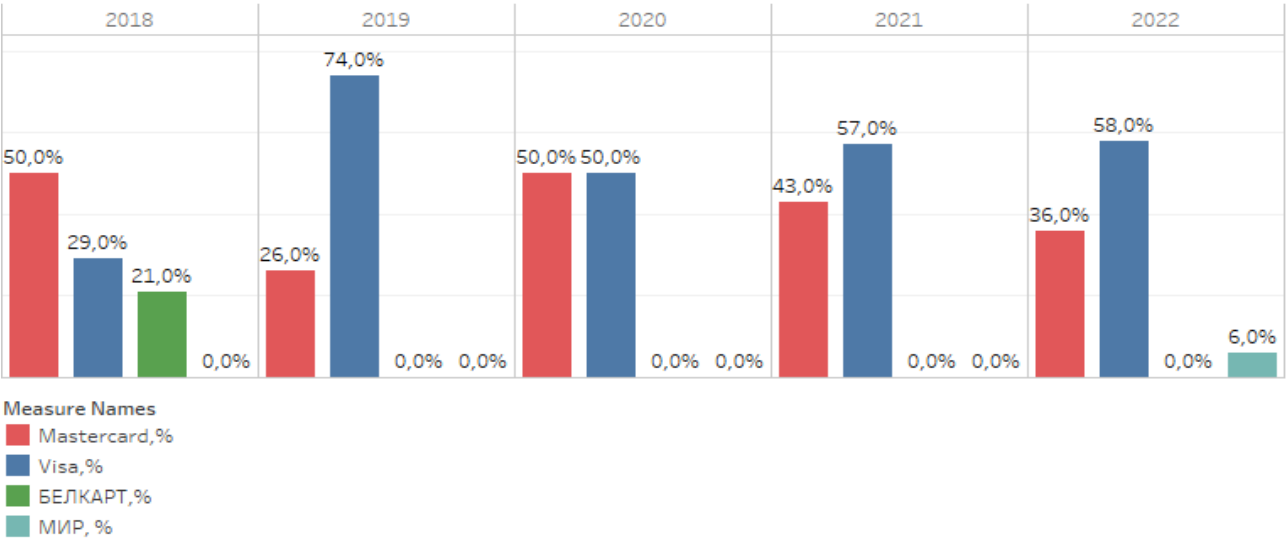
Виды мошенничества (эквайринг, условные единицы)



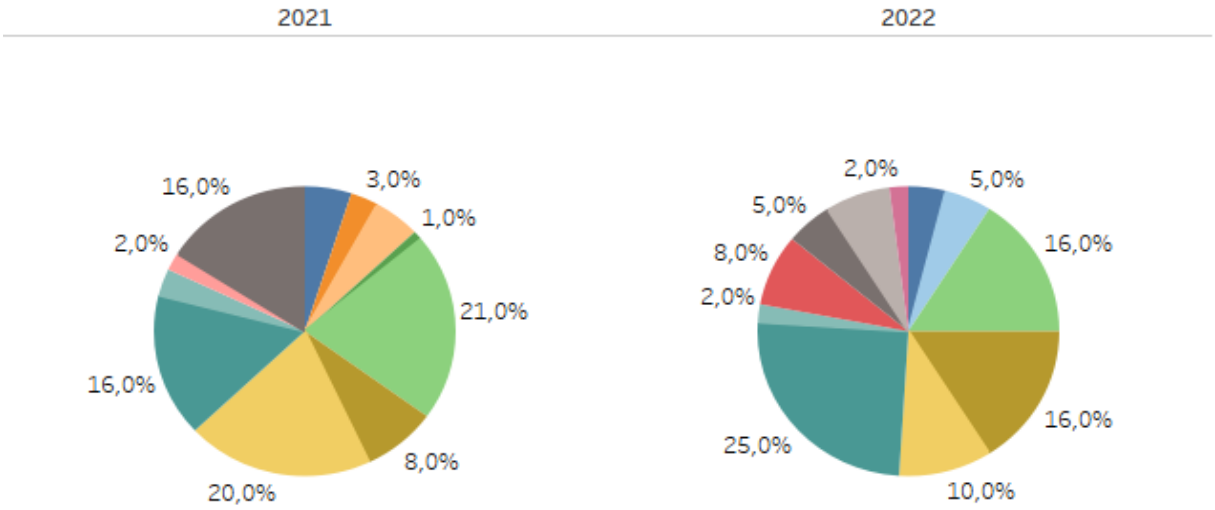
Количество мошеннических операций в разрезе мест их совершения (эквайринг, %)



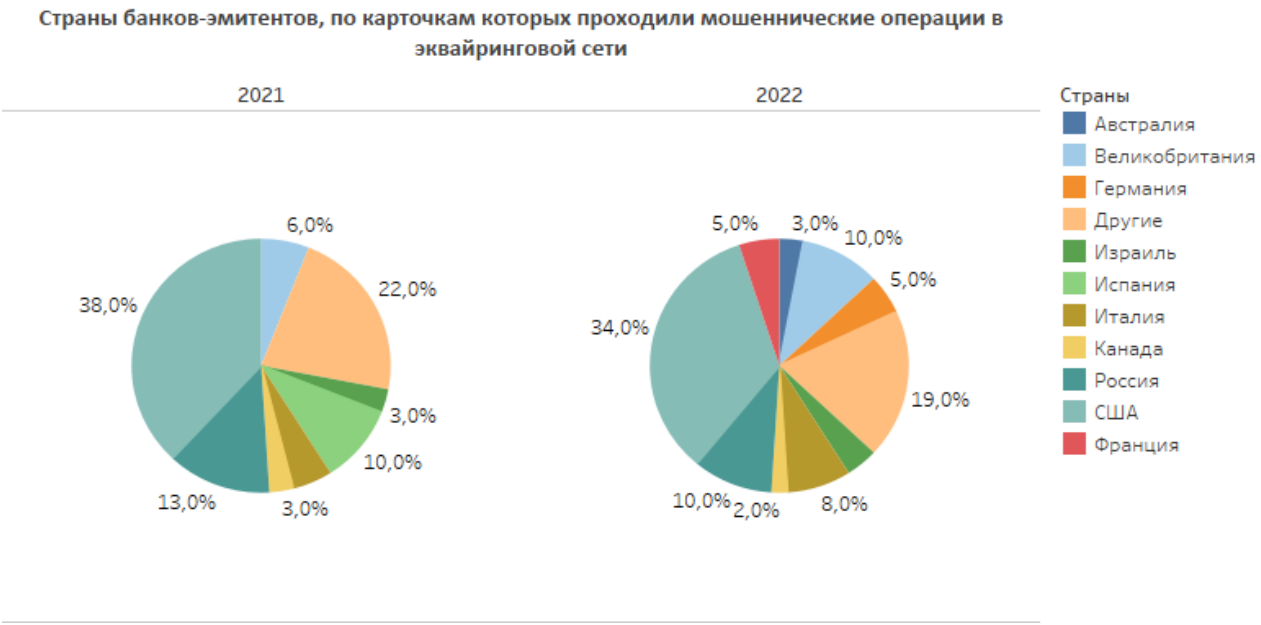
Количество мошеннических операций в разрезе платежных систем (эквайринг, %)



В каких ОТС (категориях ОТС) осуществлялись мошеннические операции в эквайерской сети по карточкам банков-нерезидентов



ОТС
- Авиакомпании
- Автозаправочные станции
- Аптеки
- Видео игры
- Гостиницы
- Другие
- Места общественного питания, рестораны и бары
- Программирование и обработка данных
- Продовольственные магазины и супермаркеты
- Профессиональные услуги
- Развлекательные услуги
- Разные товары общего назначения
- Телекоммуникационные услуги
- Услуги платного телевидения
- Услуги такси

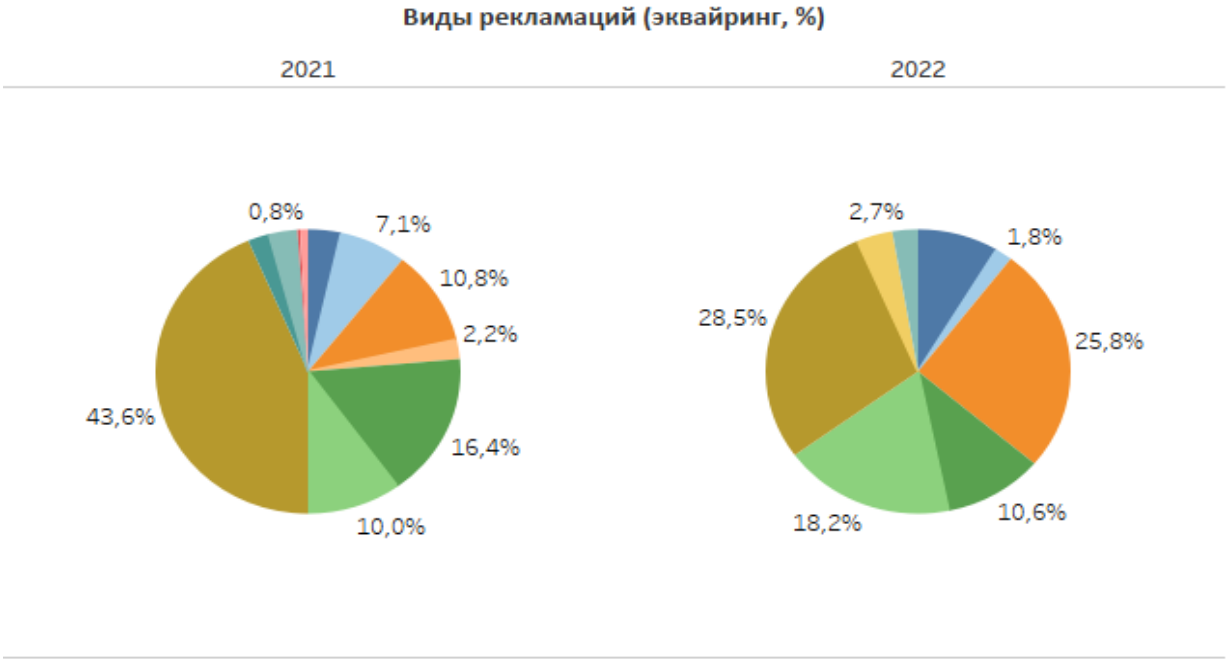


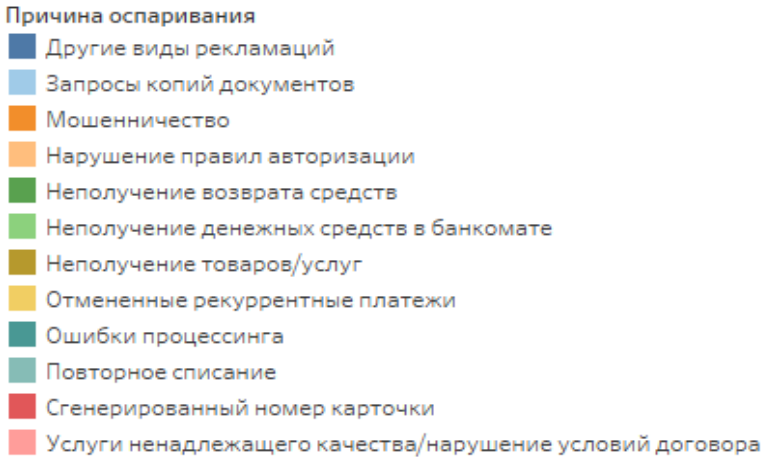
Рекламации эквайринг (данные по операциям в эквайринговой сети банков, подключенных к ОАО «Банковский процессинговый центр»):

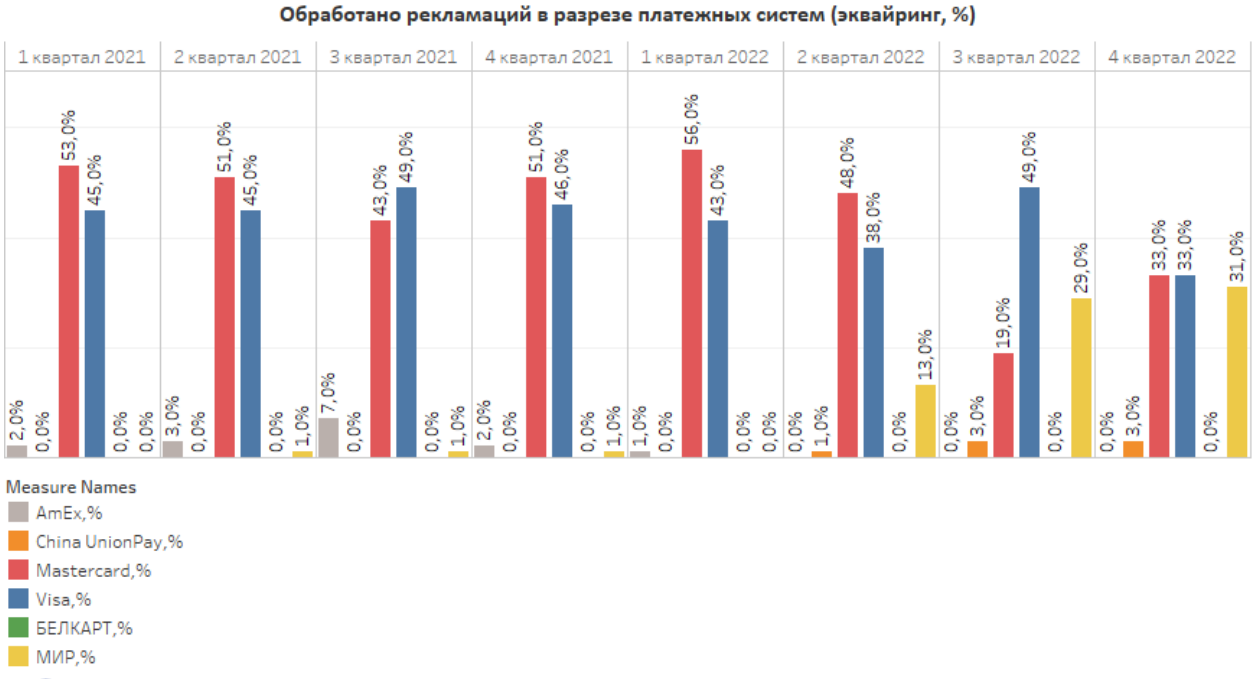
В 2022 году на 15% уменьшилось общее количество эквайерских рекламаций относительно 2021 года.

Также за отчетный год ощутимо возросло количество поступивших в адрес Общества рекламаций, инициированных по правилам ПС «Мир», и составило более 17% от общего количества поступивших рекламаций.

Детальная информация представлена на диаграммах ниже.


Виды рекламаций (эквайринг, %)
2021
2022
0,8%
7,1%
10,8%
2,2%
43,6%
16,4%
10,0%
2,7%
1,8%
28,5%
25,8%
18,2%
10,6%


Причина оспаривания
Другие виды рекламаций
Запросы копий документов
Мошенничество
Нарушение правил авторизации
Неполучение возврата средств
Неполучение денежных средств в банкомате
Неполучение товаров/услуг
Отмененные рекуррентные платежи
Ошибки процессинга
Повторное списание
Сгенерированный номер карточки
Услуги ненадлежащего качества/нарушение условий договора


Обработано рекламаций в разрезе платежных систем (эквайринг, %)
1 квартал 2021
2 квартал 2021
3 квартал 2021
4 квартал 2021
1 квартал 2022
2 квартал 2022
3 квартал 2022
4 квартал 2022
2,0% 0,0% 53,0% 45,0% 0,0% 0,0%
3,0% 0,0% 51,0% 45,0% 0,0% 1,0%
7,0% 0,0% 43,0% 49,0% 0,0% 1,0%
2,0% 0,0% 51,0% 46,0% 0,0% 1,0%
1,0% 0,0% 56,0% 43,0% 0,0% 0,0%
0,0% 1,0% 48,0% 38,0% 0,0% 13,0%
0,0% 3,0% 19,0% 49,0% 0,0% 29,0%
0,0% 3,0% 33,0% 33,0% 0,0% 31,0%
Measure Names
AmEx,%
China UnionPay,%
Mastercard,%
Visa,%
БЕЛКАРТ,%
МИР,%

Прогноз:

В соответствии с последними мировыми тенденциям мошенничество с использованием банковских платежными карточками сместилось в сферу электронной коммерции, при этом применение социальной инженерии остается на первом месте в арсенале злоумышленников. Принимая во внимание получившие популярность схемы мошенничества, можно предположить, что в 2023 году будут актуальными следующие тенденции мошенничества и угрозы в сфере безналичных платежей:

- **Социальная инженерия.** Мошенничество с использованием приемов социальной инженерии по-прежнему останется самым актуальным и масштабным. Социальная инженерия может иметь множество форм и всегда дает быстрый и эффективный результат, подстраивается под изменяющиеся экономические и геополитические условия. Злоумышленники используют различные каналы, чтобы связаться с жертвой: телефонные звонки, мессенджеры, торговые площадки, социальные сети. Мошенники очень изобретательны, поэтому гарантированно противостоять им может только сам пользователь, действуя более осознанно и с разумной осторожностью относясь к любым сообщениям и входящим звонкам.

- **Фишинговые атаки** принимают все более изощренные формы с каждым годом. Фишинговые рассылки и сайты становятся более персонализированными и их сложнее отличить от легитимных. Поддельные сайты внешне практически не отличаются от оригинальных, что усложняет задачу по их выявлению даже у продвинутых пользователей. Злоумышленники стараются приурочить фишинговые кампании к громким событиям и инфоповодам, что означает, что объемы их атак будут лишь нарастать в 2023 году.

- **Перехват доступа к СДБО и МСИ.** Данный вид мошенничества дает злоумышленникам широкий спектр возможностей, так как им становятся подконтрольны все платежные инструменты и счета держателей, появляется возможность открывать кредитные линии. Также одной из самых больших проблем будут программы удаленного доступа, которые мошенники все чаще устанавливают на мобильные устройства держателей.

- **Использование JavaScript-сниффероов в e-commerce.** В связи с постоянным развитием рынка онлайн-торговли JavaScript-сниффери представляют реальную угрозу. Пользователи онлайн-магазинов зачастую являются самым слабым звеном системы безопасности. Вводя свои платежные данные, они даже не подозревают о существовании такого типа угрозы и риске компрометации своих данных. JS-сниффер - это онлайн-аналог скиммера. Но если скиммер - миниатюрное устройство, которое перехватывает данные карточки пользователя в банкомате, то JS-сниффер - это несколько строк кода, который внедряется злоумышленниками на сайт для перехвата вводимых пользователем данных.

- **Массированные кибератаки и мошеннические атаки.** Новые масштабные скоординированные мошеннические атаки, направленные на используемые средства защиты компаниями от мошенничества, будут актуальны все чаще. Новый метод массированных атак появился во время пика праздничных распродаж – «Черной пятницы» 2022 года. Мошенники и хакеры выяснили, что лучший способ нападения – отключение технологии, с которой компании работают. Произошли многочисленные атаки на поставщиков антифрод решений, в результате чего эти системы стали временно недоступны, что привело к одобрению высокорисковых транзакций. Финансовым институтам и компаниям нужны хорошие резервные источники восстановления ПО, чтобы защитить себя от новых видов мошеннических атак.

- **Использование искусственного интеллекта.** Начинается новая эра в борьбе с мошенничеством, когда технологии искусственного интеллекта используются с двух сторон – теми, кто противостоит

злоумышленникам и самими мошенниками. Мошенники будут использовать искусственный интеллект для создания более качественных поддельных изображений и видео, которые смогут обмануть кого угодно, для создания мощных ботов, которые будут проникать через защиту бизнеса, для атак на интернет-магазины.

- **Мошенничество с подписками на игры и хищение аккаунтов.** В большинстве современных игр есть тот или иной способ монетизации: от продажи внутри игровых предметов и бустеров до внутри игровой валюты. Разумеется, все это привлекает киберпреступников, ведь игровые ценности можно продать за реальные деньги. Именно поэтому злоумышленники так активно охотятся за аккаунтами геймеров, поэтому велика вероятность появление новых схем, связанных с перепродажей виртуальных валют и имущества через хищение аккаунтов реальных пользователей.

Многие схемы мошенничества 2022 года не оказались новыми, при этом они видоизменились и подстроились под текущую ситуацию в мире, а новые технологии повлекли за собой и новые идеи мошенников, направленные на хищение денежных средств. В связи с чем всем участникам финансового рынка не стоит ожидать значительного снижения уровня мошенничества в безналичной среде и в 2023 году.